

Appl. No. 09/905,113

Amdt. Dated: May 26, 2005

Reply to Office Action of: December 7, 2004

**Amendments to the Specification**

Please replace the paragraph on line 2 of page 1 containing the title, with the following replacement paragraph:

**SYSTEM AND METHOD FOR TRUSTED BUTTON COMMUNICATION**

Please replace the paragraph on page 6, lines 14-19, with the following replacement paragraph:

The secure module 18 is adapted to operate independently of the device main processor 16, so that the internal state of the secure module 18 can not be readily reverse engineered and/or that its interactions with the underlying hardware are not maliciously intercepted and reinterpreted. The secure module 18 is programmable through appropriate toolkits to accept only certain types of instructions from underlying hardware, such as the device main processor 16. The secure module 18 can be adapted to be removably coupled to the personalized device.

Please replace the paragraph on page 6, lines 21-31, with the following replacement paragraph:

Coupled to the device main processor 16 is a device display 20, which provides textual and graphical displays that prompt a user for information input. The input of information is facilitated by a keyboard 22 coupled to the device main processor 16. Similarly, the secure module 18 is in communication with a secure display 24, a secure part of display ~~[[30]]~~ 24, and a secure input device, preferably a trusted button 26. The secure display 24 ~~[[are]]~~ is wholly under the control of the secure module 18 and coupled thereto by secure path 28, and the trusted button 26 is in direct communication with the secure module 18 via secure path 30. Thus, the secure paths 28 and 30 are logically isolated and distinct from any other paths. The secure module 18, the secure I/O devices 24 and 26, and the secure paths 28 and 30 form trusted paths between said secure module 18 and ~~[[an]]~~ a user of the personalized device 12.

**BEST AVAILABLE COPY**

Appl. No. 09/905,113

Amdt. Dated: May 26, 2005

Reply to Office Action of: December 7, 2004

Please replace the paragraph on page 7, lines 14-26 with the following replacement paragraph:

In operation, the external computer 14 assembles the data comprising the portion of the data message to be signed, preferably displaying the appropriate data message on the external display 32, and conveying the data to the personalized device 12 via the ~~transceiver 34~~ path 36. The device main processor 16 conveys the data to the secure module 18, optionally displaying the same data on the display ~~[[30]]~~ 20. The secure module 18 displays the data message, or a portion of the message, on the secure display 24 in an appropriate format. In order to verify the integrity of the data, the user compares the data message on the external display 32 and the data message, or portion of it, with the data message on the secure display 24. If there is a match between the two data messages, the user instructs the secure module 18, specifically the signature generator to generate a signature by actuating the trusted button 26. However, if the data messages differ this indicates compromise of the data message conveyed to the secure module 18 and the user can elect not to generate a signature.

BEST AVAILABLE COPY